1) A system with a B3 rating requires a trusted path:

   a) that is activated exclusively by objects.
   b) that initially identifies the TCB to a subject before it can perform any other action.
   c) to create, maintain, and protect unauthorized access.
   d) to be used for any connection between a user and the TCB.
   e) None of the above.

2) It is recommended that passwords:

   a) have a length to discourage brute force attacks.
   b) have a character range (alphanumeric, symbols) to discourageguessing.
   c) be memorable to the average user to discourage being noted on paper.
   d) All of the above.
   e) None of the above.

3) At class B2, trusted path is:

   a) not required, but recommended nevertheless.
   b) only required for logging into the system.
   c) required anytime spoofing could result in a security policy violation.
   d) required for all activity by privileged users.
   e) required for all user activity.

4) The categories “something a user knows”, “something a userhas”, and “something a user is” describe:

   a) three methods of identification.
   b) three methods of authentication.
   c) three types of passwords.
   d) None of the above.

5) The TCB must be able to:

   a) uniquely identify an individual at class C1.
   b) identify an individual’s clearance at class C2.
   c) protect authentication data from access by unauthorized users at class C1.
   d) All of the above.
   e) None of the above.

6) Which of the following statements about I&A is false for C2 and higher systems?

   a) The TCB shall protect authentication data from unauthorized access.
   b) The ability to associate the authenticated identity with all auditable events must exist.
   c) The TCB shall be able to enforce individual accountability.
   d) The TCB shall use a protected mechanism to authenticate the identity of a user.
   e) None of the above.

7) The *DoD Password Management Guideline* advocates a system that:

   a) allows users to change their own passwords.
   b) allows users to specify their own passwords.
   c) provides no information to the user about past login sessions.
   d) allows only the ISSO or the account owner to unlock an account by changing the password when an account locks due to the exceeding of the maximum lifetime of its password.
   e) All of the above.

8) Without user I&A:

   a) the mandatory access control (MAC) policy cannot be properlyenforced.
   b) the discretionary access control policy (DAC) cannot be properly enforced.
   c) the audit trail will have insufficient information to associate actions with specific users.
   d) All of the above.
   e) None of the above.

9) Group IDs are permitted as login identifiers at C1 and C2.

   a) TRUE.
   b) FALSE.

10) An ISSO is required to enter the existing password when he/she changes a user's password without the user's permission.

   a) TRUE.
   b) FALSE.